Legal 500
Country Comparative Guides 2025

Türkiye
TMT

Contributor

Hamzaoğlu
Hamzaoğlu Kınıkoğlu
Attorney Partnership

Yücel Hamzaoğlu

Partner | yucel.hamzaoglu@hhklegal.com

Batu Kınıkoğlu

Partner | batu.kinikoglu@hhklegal.com

Melike Hamzaoğlu

Partner | melike.hamzaoglu@hhklegal.com

Nur Güler

Senior Associate | nur.guler@hhklegal.com

Osman Yücel

Managing Associate | osman.yucel@hhklegal.com

This country-specific Q&A provides an overview of tmt laws and regulations applicable in Türkiye.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Türkiye: TMT

1. Software – How are proprietary rights in software and associated materials protected?

As per the Turkish law, proprietary rights in software and associated materials are protected primarily under the Law on Intellectual and Artistic Works No. 5846 ("**IP Law**") which regulates intellectual property rights. Computer programs are classified as literary works under this law, affording software the protection of copyright. This classification grants software owners exclusive rights, including the rights to process, reproduce, distribute, publicly perform, and display the software. Infringement of these exclusive rights can result in civil liability. The software owner can file a lawsuit seeking remedies such as injunctions to stop the infringing activity, monetary damages for losses incurred, and compensation for any harm suffered. The IP Law also imposes criminal liability for certain types of infringement. Unauthorised reproduction, distribution, or alteration of software can result in criminal charges, leading to penalties such as fines or imprisonment.

While registration is not required for copyright to arise, software owners have the option to register their software if they wish. Additionally, the Industrial Property Law No. 6769 covers intellectual property rights beyond copyright, including patents, utility models, and industrial designs. While copyright protects the expression of software, patents may be sought for software-related inventions that meet the patentability criteria. It is important to note that a software program itself cannot be considered an invention and would be excluded from patentability if the patent or patent application is solely related to software. However, software that is part of a broader invention that meets the criteria for patentability can be protected under this law.

In practice, the use of software is typically governed by license agreements. These agreements establish guidelines and specify terms and conditions for software use, including provisions to safeguard the software's integrity and the owner's rights. Such provisions often address issues like unauthorised copying, distribution, modification, or reverse engineering. Violating these contractual obligations can result in liability for breach of contract, with potential legal consequences.

2. Software – In the event that software is developed by a software developer, consultant or other party for a customer, who will own the resulting proprietary rights in the newly created software in the absence of any agreed contractual position?

Under the Turkish intellectual property law, specifically the Law on Intellectual and Artistic Works No. 5846 ("**IP Law**"), the default position in the absence of any agreed contractual terms is that the proprietary rights in the newly created software are owned by the software developer, consultant, or the party that created the software. According to the IP Law, the author of a work, including software, is the original owner of the copyright.

However, in scenarios where the software is developed within the scope of an employment relationship, the situation is further clarified by the Regulation on Employee Inventions, Inventions Created in Higher Education Institutions and Inventions Resulting from Public Supported Projects. According to this regulation, for software created by an employee as part of their employment duties, the employer typically holds the economic rights to the software, while the moral rights remain with the employee.

In the case of commissioned works, unless there is a specific agreement to the contrary, the copyright remains with the developer, and the customer is granted only the right to use the software as intended by the commission.

To avoid any potential disputes and ensure clarity regarding the ownership of proprietary rights in newly created software, it is essential for parties to explicitly define these terms in a written agreement. This ensures that the intended party holds the proprietary rights as per their contractual understanding.

3. Software – Are there any specific laws that govern the harm / liability caused by Software / computer systems?

In Türkiye, there are no specific legislative measures exclusively governing the harm or liability resulting from the use of software or computer systems. However, general provisions in various laws and regulations can be

applied to address such issues.

The Turkish Law of Obligations No. 6098 establishes general rules regarding liability for damages caused by acts or omissions. This framework is crucial in cases where software or computer systems cause harm, providing guidelines on determining liability and compensation for affected individuals or entities.

The Turkish Commercial Code No. 6102 plays a significant role, particularly in commercial transactions involving software. This code applies specifically to commercial activities related to software and computer systems.

The Law on Consumer Protection No. 6502 provides additional safeguards for consumers, addressing the responsibilities of manufacturers and sellers regarding defective software. Consumers have the right to repair, replacement, or refund in such cases.

The Law on the Regulation of Electronic Commerce No. 6563 imposes specific obligations on service providers and intermediaries, including those offering software. These obligations include information requirements, prohibitions on unfair commercial practices, and certain liability exemptions for intermediaries.

Sector-specific regulations may also apply, particularly in banking, finance, and healthcare, where additional rules govern the use and reliability of software systems. For instance, the Banking Regulation and Supervision Agency regulates IT systems in financial institutions.

Lastly, the Law on the Protection of Personal Data No. 6698 imposes obligations on entities processing personal data, including ensuring data security, with potential liabilities for breaches affecting data integrity and confidentiality.

4. Software – To the extent not covered by (4) above, are there any specific laws that govern the use (or misuse) of software / computer systems?

In addition to the extent covered by (4) above, the Turkish Penal Code No. 5237 contains specific provisions that address computer crimes and offenses. Turkish law provides criminal sanctions for unauthorised access to computer systems, tempering and destruction of data and other cybercrimes.

5. Software Transactions (Licence and SaaS) – Other than as identified elsewhere in this overview, are there any technology-specific laws that govern the provision of software between a software vendor and customer, including any laws that govern the use of cloud technology?

In Türkiye, there are no specific technology laws governing the provision of software between vendors and customers, so general regulations typically apply. For instance, under the Law on Intellectual and Artistic Works No. 5846 ("**IP Law**"), licensing contracts must be in written form, either physical or electronic (with e-signature by licensed Turkish entities). However, in practice, clickthrough agreements are common, particularly in SaaS models. The court of cassation has evaluated this matter, and despite the rule under the IP Law, it has often upheld the validity of clickthrough agreements due to the nature of software provision.

Furthermore, while not specifically aimed at regulating licensing and SaaS models, two pieces of legislation significantly impact related businesses in Türkiye. First, currency protection laws require that fees for locally produced software be denominated in Turkish currency. Second, the Turkish Law of Obligations No. 6098 mandates that SaaS vendors offering specialized services requiring legal or regulatory approval cannot limit their liability.

Regarding cloud services, Türkiye does not have comprehensive, specific regulations governing cloud services. However, the provisions of the Law on the Protection of Personal Data No. 6698 concerning cross-border data transfers heavily impact cloud services hosted outside Türkiye. Detailed provisions of this legislation are covered in questions 17 to 20. Despite the absence of a general regulation, various sectors have their own regulations governing cloud services, imposing standards on data handling, data residency requirements, data localisation, etc. For example, in the banking sector, the Regulation on the Information Systems of Banks and Electronic Banking Services permits limited use of cloud services but requires system localisation. In payment systems, the Communiqué on Information Systems of Payment and Electronic Money Institutions mandates data localisation and sets stringent conditions for shared cloud services, thereby limiting the involvement of conventional cloud providers. Additionally, Presidential Circular No. 2019/12 mandates that critical public sector data must be stored on systems controlled by local service providers.

These sectoral regulations illustrate the need for compliance with specific requirements depending on the

industry, emphasizing data security, localisation, and the usage of local service providers for critical data management.

6. Software Transactions (License and SaaS) – Is it typical for a software vendor to cap its maximum financial liability to a customer in a software transaction? If 'yes', what would be considered a market standard level of cap?

In Türkiye, software vendors often include clauses in contracts that limit their maximum financial liability to customers. It is uncommon to limit financial liability to foreseeable damages in Türkiye. The liability cap is typically tied to the contract's value, either as a specific amount or a percentage of the total fee. It is also common to see liability limited to the final court decision. While parties can agree on the liability cap, vendors cannot limit liability in cases of gross negligence. Additionally, as mentioned above on Q-6, under the Turkish Law of Obligations No. 6098, if a software provider offers products/services requiring expertise and legal or regulatory approval, they cannot limit their liability.

7. Software Transactions (License and SaaS) – Please comment on whether any of the following areas of liability would typically be excluded from any financial cap on the software vendor's liability to the customer or subject to a separate enhanced cap in a negotiated software transaction (i.e. unlimited liability): (a) confidentiality breaches; (b) data protection breaches; (c) data security breaches (including loss of data); (d) IPR infringement claims; (e) breaches of applicable law; (f) regulatory fines; (g) wilful or deliberate breaches.

In practice, confidentiality breaches, data protection and data security breaches, IPR infringement claims, and regulatory fines are typically excluded from the liability cap. These issues are often subject to either unlimited liability or a separate, higher cap, depending on the negotiation power of the parties.

Loss of data is generally treated as indirect damage, and software vendors often state that they are not liable for indemnifying such damages. Given that personal data protection laws impose monetary fines of up to **13.620.402 Turkish Liras** (for 2025) and considering the high risk of reputational damage (as penalty decisions and data breach notifications are published), customers often define a higher separate cap for these liabilities.

For customers in highly regulated sectors (like banking), where outsourced software use is also regulated, most of the areas of liability are typically excluded from any financial cap on the software vendor's liability.

Regarding wilful or deliberate breaches resulting from gross negligence, liability cannot be limited as per the Turkish Law of Obligations No. 6098. Therefore, such cases are not generally subject to parties' contractual discretion.

8. Software Transactions (License and SaaS) – Is it normal practice for software source codes to be held in escrow for the benefit of the software licensee? If so, who are the typical escrow providers used? Is an equivalent service offered for cloud-based software?

The escrow regime is not very common in Türkiye but is more frequently used in high-value license or SaaS relationships. Escrow arrangements provide assurance if the software vendor goes out of business, discontinues support, or breaches contractual obligations. Istanbul Technical University National Software Certification Center is the most used escrow provider in these cases.

9. Software Transactions (License and SaaS) – Are there any export controls that apply to software transactions?

There are certain export controls that apply to software transactions in Türkiye. These controls typically concern the export of specific software, technologies, or related goods to protect national security, prevent the proliferation of weapons of mass destruction, comply with international agreements, and adhere to trade sanctions or embargoes. Under the Cybersecurity Law No. 7545, which entered into force in March 2025, the export of cybersecurity-related products, systems, software, hardware, and services is subject to regulatory oversight by the Cybersecurity Directorate. Such exports must comply with procedures and principles to be set forth by the Cybersecurity Directorate, and in cases involving specified items, prior approval is required before exportation.

10. IT Outsourcing – Other than as identified

elsewhere in this questionnaire, are there any specific technology laws that govern IT outsourcing transactions?

In Türkiye, there is no specific technology law directly regulating IT outsourcing (information technology outsourcing), but various regulations may affect activities in this field. These regulations are generally considered within the framework of information security, data protection, intellectual property law, and commercial law:

- The Law on the Protection of Personal Data No. 6698 includes important regulations regarding the protection of personal data. Data processing and storage issues in IT outsourcing processes can be evaluated within the scope of this law.
- The Law on Intellectual and Artistic Works No. 5846 aims to protect software and digital content. The intellectual property rights of software and digital content developed in IT outsourcing projects can be protected by this law.
- The Turkish Commercial Code No. 6102 also affects IT outsourcing activities by governing the operations of commercial entities and incorporating regulations concerning commercial contracts, liabilities, and transactions.
- The Turkish Law of Obligations No. 6098 regulates the rights and responsibilities of the parties, the execution of obligations, liabilities, and procedures for addressing contract breaches, all of which are critical aspects of IT outsourcing agreements.

In addition to general regulations, there are also some sector-specific regulations. For example, there is a regulation concerning the procurement of support services related to the outsourcing of banks. This regulation is issued by the Banking Regulation and Supervision Agency, and in accordance with this regulation, banks must adhere to specific rules when obtaining IT services from external sources. Another regulation is found in the Communiqué on Information Systems of Payment and Electronic Money Institutions and Data Sharing Services in the Field of Payment Services by Payment Service Providers, which stipulates conditions for IT outsourcing services due to sectoral sensitivities in the management of information systems. In addition, the Ministry of Industry and Technology has introduced a certification scheme requiring companies wishing to participate in public IT procurements to obtain specific authorisation certificates, such as the Public IT Authorisation Certificate, Software Authorisation Certificate, or Penetration Testing Authorisation Certificate. Similarly, the Insurance and Private Pension Regulation and Supervision Agency has imposed requirements on insurance and pension companies outsourcing their IT systems, particularly regarding data integrity, cybersecurity, and backup obligations.

11. IT Outsourcing – Please summarise the principal laws (present or impending), if any, that protect individual staff in the event that the service they perform is transferred to a third party IT outsource provider, including a brief explanation of the general purpose of those laws.

In Türkiye, there are no specific legal regulations dedicated solely to the outsourcing of services to a third-party IT provider. Generally, the Labor Law No. 4857 protects the rights of individual employees. This law regulates various aspects of employment relationships and provides certain protections to employees in cases of business transfer or change of employer. In the event of transferring a service to a third-party IT outsourcing provider, the law aims to protect the rights of employees and maintain employment relationships. The acquiring party cannot terminate existing employment contracts solely based on the transfer itself. Employment contracts remain valid upon transfer of the workplace. However, after acquiring the workplace, the new employer may terminate employment contracts if there are operational reasons or restructuring needs, but such reasons must be genuine.

Additionally, for a period of two years from the date of transfer, the former employer remains jointly liable with the new employer towards the employees. Moreover, if the new employer terminates the employment without valid reason, the employee can claim job security and not only entitlement to compensation but also the right to request reinstatement under the same conditions and can also claim their rights from the former employer.

12. Telecommunications – Please summarise the principal laws (present or impending), if any, that govern telecommunications networks and/or services, including a brief explanation of the general purpose of those laws.

The primary legislation overseeing telecommunications networks and services is the Electronic Communications Law No. 5809 ("**Law No. 5809**"). This law encompasses the regulation of electronic communications services, the development and management of the necessary infrastructure, and the associated network systems. Additionally, it governs the production, importation, sale, construction, and operation of various electronic

communications equipment and systems.

In addition to Law No. 5809, a significant legislative development is the entry into force of the Cybersecurity Law No. 7545 in March 2025. This new law introduces comprehensive cybersecurity requirements across sectors deemed critical to national infrastructure — including the telecommunications industry, which will be classified as a critical infrastructure sector. It imposes obligations on network operators and service providers, particularly in areas such as data security, risk assessment, asset inventory management, and compliance auditing.

In addition to the above, there are also several secondary regulations that support the primary legislation. The most notable of these secondary regulations include the following:

- Internet Domain Names Regulation,
- Regulation on Consumer Rights in the Electronic Communication Sector,
- Regulation on Quality of Service in the Electronic Communication Sector,
- Regulation on Network and Information Security in the Electronic Communications Sector,
- Regulation on Authorisation for the Electronic Communication Sector,
- Regulation on the Processing of Personal Data and Protection of Privacy in the Electronic Communications Sector,
- Regulation on the Process of Verifying the Identity of the Applicant in the Electronic Communication Sector,
- Radio Equipment Regulation,
- Regulation on Market Surveillance and Inspection of Radio and Telecommunication Terminal Equipment,
- Regulation on Security Certificate for Electronic Communication Devices,
- Regulation on Emergency Aid Call Services in the Electronic Communication Sector,
- Number Portability Regulation,
- Regulation on Electronic Communication Infrastructure and Information System,
- Information Technologies and Communication Authority Regulation on Administrative Sanctions,
- Communiqué on Procedures and Principles for Obtaining Electromagnetic Field Measurement Certificate,
- Communiqué on Obtaining Service Quality Criteria for 3N Mobile Communication Services,
- Communiqué on Notification of Devices Produced, Manufactured or Assembled in Türkiye,
- Communiqué on Obtaining Service Quality Measures for GSM Mobile Telephony Services,
- Communiqué on the Registration of Devices with Electronic Identity Information.
- Draft Regulation on the Provision of Over-the-Top (OTT) Services
- Draft Communiqué on Ecodesign Requirements for Smartphones, Mobile Phones Other Than Smartphones, Cordless Phones and Tablets
- Draft Regulation Amending the Radio Equipment Regulation (2014/53/EU)

13. Telecommunications – Please summarise any licensing or authorisation requirements applicable to the provision or receipt of telecommunications services in your country. Please include a brief overview of the relevant licensing or authorisation regime in your response.

In Türkiye, the provision of electronic communications services and the operation of related infrastructure and networks are regulated primarily under the Electronic Communications Law No. 5809 ("**ECL**") and the secondary legislation issued by the Information and Communication Technologies Authority ("**ICTA**"). Any entity intending to offer electronic communication services or to establish and operate electronic communications networks or infrastructure is required to obtain prior authorisation from ICTA.

Authorisation is structured around a general authorisation regime based on notification. Entities that do not require the allocation of scarce public resources—such as frequency bands, numbering plans, or satellite positions—are authorized through a notification procedure. In this context, companies notify ICTA by submitting the required information on the nature of the services, technical infrastructure, and geographical scope. Upon approval and issuance of an authorisation certificate, the operator may commence service provision and/or network operation within the notified scope.

Where the intended service involves the use of scarce resources, the notification must be followed by the acquisition of usage rights from ICTA. In both cases, the operator is granted the right to offer services or operate infrastructure only within the limits of the authorisation issued. In addition to the general notification process, companies must meet certain additional requirements to qualify for authorisation. These include being established as a limited or joint stock company, including the requested electronic communication activity within the scope of the company's articles of association, and ensuring that shareholders holding a significant portion of shares and company executives have no criminal

convictions for specific offenses. Furthermore, the company must meet the minimum paid-in capital threshold determined by ICTA.

Authorised operators are subject to several regulatory obligations, including compliance with consumer protection rules, ensuring service continuity and network security, fulfilling data retention and lawful interception requirements, and paying annual regulatory fees and contributions to the universal service fund, where applicable. Moreover, any change in the operator's corporate structure, shareholding, or control that may impact regulatory compliance must be notified to ICTA, and in certain cases, prior approval is required. Authorisation durations vary depending on the type of service and may be renewed upon expiration.

Overall, the Turkish authorisation regime covers a broad array of electronic communication activities, including the transmission and receipt of data signals, operation of infrastructure and networks, and the provision of services, each of which falls within ICTA's defined scope of electronic communication.

14. Telecommunications – Please summarise the principal laws (present or impending) that govern access to communications data by law enforcement agencies, government bodies, and related organisations. In your response, please outline the scope of these laws, including the types of data that can typically be requested, how these laws are applied in practice (e.g., whether requests are confidential, subject to challenge, etc.), and any legal or procedural safeguards that apply.

The principal legislation governing access to communications data in Türkiye is the Electronic Communications Law No. 5809, which sets out comprehensive rules on the processing, retention, and protection of such data, and outlines the conditions under which it may be accessed by competent authorities.

Under this framework, operators must retain traffic, location, and subscriber identity data for one to two years, depending on the data type. However, the confidentiality of communications and traffic data is a fundamental principle, and unless explicitly authorised by applicable legislation or judicial decisions, any listening to, recording, storing, interception, or monitoring of communications without the consent of all parties involved is strictly prohibited.

The primary regulation detailing lawful interception is the Regulation on the Procedures and Principles for Detection, Listening to, Evaluation and Recording of Communications Made Through Telecommunications and the Establishment, Duties and Authorities of the Telecommunications Communication Presidency ("**Regulation**"), published in Official Gazette No. 25989 on 10 November 2005. This Regulation prohibits anyone from intercepting or recording communications unless done in full compliance with its procedures. It distinguishes two categories of interception: (i) preventive or intelligence-based measures, and (ii) judicially authorized measures under the Criminal Procedure Code No. 5271 ("**Criminal Procedure Code**").

Preventive measures may be used in cases of national security or public order threats and, in urgent situations, initiated by senior officials from the National Intelligence Organisation (MIT) or the Security General Directorate, subject to judicial approval within 24 hours. If judicial approval is not granted within this timeframe, the interception measure must be immediately terminated. Also, these measures may be authorized for up to three months, with limited extensions.

In contrast, judicially authorised interception under the Criminal Procedure Code is available in the context of a criminal investigation or prosecution and may only be permitted when there is strong suspicion that a crime has been committed and no other means exist to obtain the necessary evidence. A judge may then authorise the monitoring, interception, recording, and evaluation of telecommunications involving the suspect or defendant. In urgent circumstances, a public prosecutor may issue a temporary order, but it must be submitted to a judge within 24 hours for approval. If the order is not confirmed, or the deadline lapses, the interception must be immediately revoked. These measures are strictly limited to serious offences known as "catalogue crimes" under Article 135 of the Criminal Procedure Code, including crimes against national security, armed organisation membership, terrorism, narcotics trafficking, organised smuggling, money laundering, corruption, child sexual abuse, and espionage or offences against state secrets.

Depending on the nature and legal basis of the measure authorized under the Regulation, competent authorities may access not only the content of communications (such as voice calls or data transmitted via telecommunication networks), but also associated metadata, including call and connection logs, location data, and identity information.

Interception measures must follow strict procedures, be limited in scope and duration, and remain confidential.

Judicial orders and authorisations are classified and not shared with telecom operators or individuals under surveillance. All related activities are likewise confidential. As part of the legal and procedural framework, all interception decisions are subject to prior or post-authorisation by a judge, thereby providing an essential ongoing check on executive power. While the Regulation does not grant individuals the right to be notified of surveillance measures or to challenge them in advance, if intercepted data is introduced as evidence in criminal proceedings, the defendant may contest its admissibility on grounds such as illegality or procedural impropriety, in line with general principles of Turkish criminal law and due process.

15. Mobile communications and connected technologies – What are the principle standard setting organisations (SSOs) governing the development of technical standards in relation to mobile communications and newer connected technologies such as digital health or connected and autonomous vehicles?

Although the Turkish Standards Institution ("**TSE**") was established to develop standards for various products, processes, and services in Türkiye, there is not a single main SSO that sets principles for all new connected technologies. Instead, multiple institutions govern the development of technical standards in their respective areas.

For mobile communications, the Information and Communication Technologies Authority ("**ICTA**") is the primary SSO responsible for setting principles. The ICTA was established to ensure that the regulation and supervision of the telecommunications sector are conducted by an independent administrative authority. Additionally, the ICTA mandates several standards related to connected and autonomous vehicles, focusing on mobile services, network usage, and connected services within these vehicles.

Examples of other institutions include the Ministry of Transport and Infrastructure ("**Ministry**"), which serves as the main SSO for connected and autonomous vehicles, setting relevant principles and standards. The Ministry is operating Open Innovation Autonomous Vehicle Development and Test Platform to support local R&D and compliance testing infrastructure. In parallel, the Ministry recently released a national report on connected vehicle testing, highlighting that by 2030, Türkiye aims to finalise the legal framework for autonomous driving, including rules on data security, liability, insurance, and road integration procedures.

For digital health services, the Turkish Medicines and Medical Devices Agency, operating under the Ministry of Health, is the primary SSO responsible for setting principles and standards in this area.

16. Mobile communications and connected technologies – How do technical standards facilitating interoperability between connected devices impact the development of connected technologies?

While there are no specific laws in Türkiye that exclusively regulate interoperability, various regulations and standards indirectly ensure that interoperability is maintained within the realm of electronic communications and connected technologies. Interoperability in mobile communications and connected technologies is primarily ensured through a combination of regulations and standards set by the Information and Communication Technologies Authority ("**ICTA**") and the Turkish Standards Institution ("**TSE**"). The ICTA mandates that network operators interconnect their networks and follow specific technical standards to maintain seamless communication services. Additionally, the TSE develops and publishes national standards which ensure that devices like Wi-Fi routers and Bluetooth equipment operate compatibly and without interference.

Moreover, Türkiye often aligns its regulations with the European Union directives, which also promote interoperability. For instance, the Radio Equipment Directive 2014/53/EU and the EU's General Data Protection Regulation influence Turkish regulations by encouraging the development of interoperable systems.

17. Data Protection – Please summarise the principal laws (present or impending), if any, that that govern data protection, including a brief explanation of the general purpose of those laws.

The principal legislation governing data protection in Türkiye is the Law on the Protection of Personal Data No. 6698 ("**LPPD**"), dated April 7, 2016. This law, primarily based on EU Directive 95/46/EC, aims to protect the privacy of individuals by regulating the processing of personal data.

Similar to EU's the General Data Protection Regulation ("**GDPR**"), the LPPD aims to protect personal privacy and to ensure data security by regulating the obligations and

principles for individuals and organisations that process personal data. In addition to these goals, the LPPD is designed to stop the unrestricted and random gathering of personal data, prevent unauthorised access, and avoid its disclosure or misuse, which could result in violations of personal rights.

Several secondary regulations have been enacted to implement various aspects of the LPPD, including:

1. **Regulation on the Erasure, Destruction, and Anonymizing of Personal Data** (published in the Official Gazette on October 28, 2017, numbered 30224): Outlines the methods and principles for deleting, destroying, and anonymizing personal data.
2. **Regulation on the Registry of Data Controllers** (published in the Official Gazette on December 30, 2017, numbered 30286): Establishes the rules for the registration of data controllers.
3. **Communiqué on Procedures and Principles for Compliance with the Obligation to Inform** (published in the Official Gazette on March 10, 2018, numbered 30356): Sets the guidelines for data controllers to inform data subjects about data processing activities.
4. **Communiqué on the Principles and Procedures for Requests to Data Controllers** (published in the Official Gazette on March 10, 2018, numbered 30356): Outlines how data subjects can request information from data controllers.
5. **Regulation on the Procedures and Principles Regarding the Transfer of Personal Data Abroad** (published in the Official Gazette on July 10, 2024, numbered 32598): Outlines the rules and principles applicable to the cross-border transfer of personal data.

Apart from these secondary regulations, the Turkish Data Protection Authority ("**TDPA**") regularly issues and publishes its decisions and principle decisions to clarify specific issues and provide guidance for data controllers and processors on how to implement such rules regarding data protection, including:

1. **Decision of the Data Protection Board on Adequate Measures for Processing Special Categories of Personal Data** (dated January 31, 2018, numbered 2018/10): Specifies the additional measures data controllers must take when processing special categories of personal data.
2. **Decision of the Data Protection Board on Personal Data Breach Notification Procedures and Principles** (dated January 24, 2019, numbered 2019/10): Specifies the procedure and the time period on how to notify the TDPA and data subjects in case of data breach, including the form to be used for the notification.

Alongside its decisions, the TDPA also releases various guidelines to offer guidance on different matters. The most notable ones include:

1. Guideline on Personal Data Security (Technical and Organisational Measures),
2. Guideline on the Processing of Special Categories of Personal Data
3. Guideline on the Transfer of Personal Data Abroad
4. Guideline on Preparation of the Data Inventory,
5. Guideline on Implementation of the Obligation to Inform,
6. Guideline on Erasure, Destruction and Anonymisation of Personal Data,
7. Recommendations for Protecting Privacy in Mobile Applications,
8. Guide on Protection of Personal Data – Banking Sector Good Practices,
9. Guide on Protection of Personal Data – Payment and E-Money Sector Good Practices,
10. Guide on Cookie Practises,
11. Guide on the Right to be Forgotten (Evaluation of the Right to be Forgotten Specific to Search Engines).
12. Guide on the Issues to Be Considered When Processing Biometric Data,
13. Guide on the Issues to Be to be Considered When Processing Genetic Data,
14. Recommendations on the Protection of Personal Data in the Field of Artificial Intelligence.

The general purpose of these laws and regulations along with decisions and guidelines is to safeguard personal data, ensure data privacy, and establish clear guidelines for data processing activities within Türkiye. It is also important highlight here that one of the goals stated in Türkiye's Medium-Term Programme (2024-2026), published by the Turkish Presidential Strategy and Budget Directorate, is to ensure the alignment of data protection law with EU legislation, particularly the GDPR. In accordance with this goal, amendments were made to the LPPD on June 1st 2024. The amendments have introduced new mechanisms for the transfer of personal data abroad, in close alignment with those of the EU. The rules on the processing of special categories of personal data have also been updated to address challenges encountered in practice.

In addition to those mentioned earlier, various regulations specify rules and requirements for processing personal data in sectors such as banking and finance, health, and electronic communications.

18. Data Protection – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable data protection laws?

In the event of a breach of applicable data protection laws in Türkiye, the maximum administrative fine foreseen for 2025 is **13,620,402 Turkish Liras**. It is important to note that the number of administrative fines stated in the Law on the Protection of Personal Data No. 6698 is increased every year at the rate of revaluation.

19. Data Protection – Do technology contracts in your country typically refer to external data protection regimes, e.g. EU GDPR or CCPA, even where the contract has no clear international element?

In Türkiye, technology contracts generally do not refer to external data protection regimes like the EU GDPR or CCPA when there is no clear international element involved. When both parties are established in Türkiye, these contracts almost exclusively refer to the Law on the Protection of Personal Data No. 6698. However, when one of the parties is established outside of Türkiye, references to different data protection regimes, especially EU GDPR, can be seen.

20. Cybersecurity – Please summarise the principal laws (present or impending), if any, that that govern cybersecurity (to the extent they differ from those governing data protection), including a brief explanation of the general purpose of those laws.

The principal legislation governing cybersecurity in Türkiye is the Cybersecurity Law No. 7545 ("**Cybersecurity Law**"), enacted on March 19, 2025. As the first comprehensive legal framework in this area, the Cybersecurity Law consolidates previously fragmented, sector-specific regulations into a unified regime and establishes a broad regulatory structure applicable to all individuals and entities operating in cyberspace.

The implementation and oversight of the Law are entrusted to two key authorities: the Cybersecurity Council, responsible for defining the national cybersecurity strategy, policies, and action plans; and the Cybersecurity Directorate ("**the Directorate**"), tasked with executing these strategies and ensuring regulatory compliance.

Entities operating in the cybersecurity field are subject to authorisation, certification, and accreditation requirements, which must be fulfilled within one year following the issuance of the secondary legislation. Non-compliance may result in suspension of activities or, in the case of companies, liquidation.

One of the core aspects of the Cybersecurity Law is that it introduces stricter requirements for entities considered part of **critical infrastructure**. These entities are obliged to maintain detailed inventories of their assets, including data assets, conduct risk assessments, and implement appropriate cybersecurity measures aligned with the criticality of each asset. Although the Law does not provide a specific list, sectors such as energy, transportation, telecommunications, public services, and finance are expected to be designated as critical infrastructure by the Cybersecurity Council.

The Cybersecurity Law also imposes export controls on cybersecurity products, systems, software, hardware, and services, which may be subject to prior approval or evaluation, as determined by the Directorate. Corporate transactions such as mergers, demergers, and share transfers involving cybersecurity companies must be reported to the Directorate, with certain transactions requiring prior authorisation. The Directorate is further empowered to conduct both scheduled and ad hoc audits, perform inspections, and request technical information and system data where necessary.

Moreover, the Cybersecurity Law establishes a mandatory notification regime for cybersecurity incidents and vulnerabilities. Any breach of the confidentiality, integrity, or availability of information systems—or identification of a significant vulnerability—must be reported to the Directorate without delay.

As the Cybersecurity Law has only recently entered into force, the secondary legislation—expected within one year—is awaited to provide detailed guidance on implementation and compliance obligations.

21. Cybersecurity – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable cybersecurity laws?

In the event of a breach of the Cybersecurity Law No. 7545 in Türkiye, violations may result in severe legal consequences, including prison sentences of up to 15 years. In addition, entities may face substantial administrative fines. For 2025, the maximum administrative fine is set at 100,000,000 Turkish Liras, or

up to 5% of a company's gross annual revenue.

22. Artificial Intelligence – Which body(ies), if any, is/are responsible for the regulation of artificial intelligence?

Although there is no body directly responsible for the regulation of artificial intelligence ("**AI**") in Türkiye, it is important to note here that Türkiye's approach is currently evolving to AI governance. Following the establishment of the Department of Big Data and AI Applications within the Digital Transformation Office of The Presidency of The Republic of Türkiye, a crucial initiative was the formulation of a national strategy aimed at regulating interactions with AI. Therefore, it is envisioned that in the future there may be a specialized and singular authority, akin to the Turkish Data Protection Authority ("**TDPA**"), solely responsible for AI regulations. Moreover, specific governmental organisations and administrative authorities may regulate particular issues that fall within their authorisation. For example, the Information and Communication Technologies Authority ("**ICTA**") can establish rules regarding the use of AI in the telecommunications sector, while the TDPA can oversee how AI processes personal data. In addition, the Turkish Grand National Assembly established an AI Research Commission which began working on a comprehensive report to assess regulatory needs and explore the possible creation of a central coordinating AI authority, potentially similar to the TDPA.

23. Artificial Intelligence – Please summarise the principal laws (present or impending), if any, that that govern the deployment and use of artificial intelligence, including a brief explanation of the general purpose of those laws.

Currently, Türkiye lacks a comprehensive law specifically governing and focusing the deployment and utilisation of artificial intelligence, like the EU's AI Act. Given that AI is swiftly reshaping numerous sectors worldwide, Türkiye is also witnessing significant transformations. Consequently, there is growing momentum towards regulating AI systems.

Additionally, some references to the use of AI technologies, such as deep fakes, can be seen in some sectoral legislations. For instance, as per the Communiqué on Remote Identification Methods to Be Used By Intermediary Institutions and Portfolio Management Companies and on the Establishment of Contractual Relationships In Electronic Environment, intermediary institutions or portfolio management companies must take additional measures to prevent risks related to deepfake technology.

Additionally, governmental organisations and administrative authorities have developed specific strategies and guidelines pertaining to AI:

- The National Artificial Intelligence Strategy 2024–2025 Action Plan of Türkiye outlines a comprehensive roadmap to strengthen the country's position in the global AI landscape. Developed collaboratively by the Ministry of Industry and Technology and the Presidential Digital Transformation Office, the plan is structured around six strategic priorities: developing talent, fostering innovation, improving infrastructure, promoting responsible AI use, enhancing international cooperation, driving institutional transformation.
- Within the scope of processing personal data by AI systems, the Turkish Data Protection Authority has also issued a guideline, namely the Recommendations on the Protection of Personal Data in Artificial Intelligence, which outlines its stance and provide general guidance on safeguarding personal data in the use of AI-driven technologies. These recommendations are intended for developers, manufacturers, service providers, and decision-makers in the AI sector.

24. Artificial Intelligence – Are there any specific legal provisions (present or impending) in respect of the deployment and use of Large Language Models and/or generative AI (including agentic AI)?

In Türkiye, there are currently no specific legal provisions governing the deployment and utilisation of Large Language Models ("**LLMs**") and/or generative AI ("**GenAI**"). However, the Council of Higher Education ("**CoHE**") has issued guidance regarding the use of GenAI in scientific research conducted by higher education institutions.

The Ethical Guidelines on the Productive Use of Artificial Intelligence in Scientific Research and Publication Activities of Higher Education Institutions, published by the CoHE in 2024, outline principles for the ethical and effective utilisation of LLMs and GenAI in scientific research and related activities. These guidelines serve to establish standards and foundational principles for the responsible deployment of LLMs and GenAI in academic settings, ensuring their ethical use and promoting integrity in research practices. Furthermore, the updated

the National Artificial Intelligence Strategy (2024–2025 Action Plan) includes objectives to establish ethical and technical standards for GenAI systems, and TÜBİTAK and the Turkish Standards Institution have begun preparatory work in this area.

25. Artificial Intelligence – Do technology contracts in your jurisdiction typically contain either mandatory (e.g. mandated by statute) or recommended provisions dealing with AI risk? If so, what issues or risks need to be addressed or considered in such provisions?

No, currently in Türkiye, technology contracts generally do not include mandatory or recommended provisions addressing AI risks. However, given Türkiye's developing stance on AI regulation, this may change in the future.

26. Artificial Intelligence – Do software or technology contracts in your jurisdiction typically contain provisions regarding the application or treatment of copyright or other intellectual property rights, or the ownership of outputs in the context of the use of AI systems?

Yes, software and technology contracts in Türkiye increasingly include provisions addressing the ownership and use of outputs generated by AI systems, particularly in agreements involving **generative AI** tools. As the use of AI becomes more widespread, contracting parties are more frequently negotiating and explicitly defining who holds the intellectual property rights over AI-generated outputs, under what circumstances such outputs may be used, and whether any limitations or licensing terms apply.

These clauses typically aim to clarify whether the outputs will be owned by the user, the service provider, or jointly, depending on factors such as the nature of the AI system, the degree of human input, and the terms of the underlying software license. In many cases, contracts also address related concerns such as data ownership, the use of training datasets, confidentiality, liability, and warranties regarding the originality and non-infringement of AI-generated content.

27. Blockchain – What are the principal laws (present or impending), if any, that govern (i) blockchain specifically (if any) and (ii) digital assets, including a brief explanation of the general purpose of those laws?

In Türkiye, there is currently no specific legislation dedicated solely to regulating blockchain technology and digital assets. However, crypto assets and crypto asset service providers ("**CASPs**") are regulated through the Capital Markets Law ("**CML**"). The CML covers the issuance of crypto assets, the establishment and commencement of operations by CASPs, and the requirement to obtain permits from the Capital Markets Board ("**CMB**"). It also specifies the conditions that partners of CASPs must meet, the obligations these providers must adhere to during their operations, the activities of platforms, and the transactions Turkish residents can perform on these platforms, including trading and transferring crypto assets.

Additionally, the CML addresses crypto asset custody services, the safeguarding of clients' cash assets, the prohibition of market disruptive actions, auditing, liability of CASPs for damages, seizure of customers' crypto assets, dispute resolution, administrative penalties, operational measures, fees payable to the CMB, transitional and compliance processes, and penal provisions. The CMB has been empowered to regulate CASPs, granting it authority to issue specific and general decisions, enforce measures, and impose sanctions.

CASPs are required to obtain a license from the CMB before they can be established and commence operations. The CMB is also responsible for detailing regulations concerning the organisational structures, capital adequacy, and technological infrastructures of CASPs, among other aspects. Any contractual terms that absolve CASPs from their responsibilities towards clients are deemed void. A legal framework has been established with regard to the seizure of crypto assets owned by customers, ensuring their enforceability by CASPs. CASPs are exclusively subject to the stipulations outlined in the relevant provisions concerning crypto assets and are not governed by the remaining parts of the CML.

Additionally, the Regulation on Measures for the Prevention of Laundering Proceeds of Crime and Financing of Terrorism includes CASPs among the obliged parties. Consequently, CASPs are now required to fulfill fundamental obligations such as know-your-customer (KYC) standards and reporting suspicious transactions as part of efforts to prevent money laundering and terrorism financing.

Furthermore, the regulatory framework for CASPs is complemented by secondary regulations such as the Communiqué Regarding Principles on the Establishment

and Operation of Crypto Asset Service Providers, the Communiqué Regarding Operating Procedures and Principles and Capital Adequacy of Crypto Asset Service Providers, and the Communiqué on Procedures and Principles Regarding Information Systems Management, which elaborate on structural, procedural, financial, and technological standards applicable to CASPs.

28. Search Engines and Marketplaces – Please summarise the principal laws (present or impending), if any, that govern search engines and marketplaces, including a brief explanation of the general purpose of those laws.

There is currently no specific legislation exclusively regulating search engines in Türkiye. However, certain aspects of existing legal frameworks apply to search engine activities. For example, the Industrial Property Law No. 6769 prohibits the use of third-party registered trademarks as advertising keywords on search engines, deeming such use as trademark infringement and therefore unlawful. Similarly, the Law No. 5651 on the Regulation of Broadcasts via Internet and Prevention of Crimes Committed through Such Broadcasts ("**Internet Law**") may apply in limited contexts, particularly where content liability or access restrictions are at issue.

The right to be forgotten has also been recognized by the Turkish judiciary, especially through the decisions of the court of cassation. In line with these precedents, the Turkish Data Protection Authority published the Guide on the Right to be Forgotten (Evaluation of the Right to be Forgotten Specific to Search Engines), which outlines how individuals may request delisting from search results. In addition, the Advertising Board is authorized to investigate complaints concerning unfair commercial practices related to search engine advertisements and may impose access restrictions when deemed necessary.

Marketplaces, on the other hand, are governed by a more comprehensive regulatory framework. Under the Internet Law, marketplaces may be classified as "hosting providers," defined as real or legal persons that provide or operate systems containing services or content. In this context, marketplaces are obliged to remove illegal content once notified.

The primary legislation regulating marketplaces is the Law on the Regulation of Electronic Commerce No. 6563 ("**Law No. 6563**") and the Regulation on Electronic Commerce Intermediary Service Providers and Electronic Commerce Service Providers ("**E-Commerce Regulation**"). Law No. 6563 outlines the obligations of electronic commerce intermediary service providers ("**EISPs**") and electronic commerce service providers ("**ESPs**"), their relationships with consumers, and rules on advertising, commercial communication, and unfair commercial practices. It also defines key concepts such as economic integrity and net transaction volume. The E-Commerce Regulation complements this law by setting forth more detailed requirements, particularly obligations that vary based on the provider's transaction volume and scale. It also outlines the supervisory powers of the Ministry of Trade and the interrelations between EISPs and ESPs.

As of January 1, 2025, there is a mandatory licensing regime for electronic commerce in Türkiye. EISPs and ESPs are now required to obtain a license if their annual net transaction volume and transaction count exceed prescribed thresholds. Failure to comply with licensing obligations may result in administrative sanctions imposed by the Ministry of Trade.

In addition to the above, several secondary regulations govern e-commerce activities, including those related to distance contracts, pricing, unfair terms in consumer agreements, advertising, unfair commercial practices, trust stamps in e-commerce, and commercial communication. Furthermore, general laws such as the Consumer Protection Law, the Law on the Protection of Personal Data No. 6698, the Law on Bank Cards and Credit Cards, as well as the secondary legislation enacted under these laws and the decisions of the Advertising Board, are applicable to e-commerce activities where relevant.

29. Social Media – Please summarise the principal laws (present or impending), if any, that govern social media and online platforms, including a brief explanation of the general purpose of those laws?

In Türkiye, social media is mainly regulated by the Law No. 5651 on the Regulation of Broadcasts via Internet and Prevention of Crimes Committed through Such Broadcasts ("**Internet Law**") as well as some secondary legislation. The Internet Law defines social network provider as "natural persons or legal entities that enable users to create, display or share content such as texts, image, voice, location, over the internet for purposes of social interaction" and lay down some obligations for social network providers having more than one million daily access from Türkiye:

- Appointment of local representative for social network providers having more than one million daily access

from Türkiye, and notifying the representative to Information and Communication Technologies Authority ("**ICTA**"),
- Removing content or blocking access to content, when necessary (such as violation of personal rights or privacy),
- Providing necessary information upon request of public institutions and/or judicial authorities, and
- Act in compliance with decisions of the ICTA.

Additionally, the Procedures and Principles on Social Network Providers published by the ICTA also lay down the details of aforementioned obligations such as appointment of representative, reporting, hosting of data in Türkiye, responding applications, informing the judicial authorities, protecting users' rights and procedures to ensure compliance in detail.

Additionally, in cases where the social network provider is a qualified as a hosting provider, the social network provider is obliged to act in accordance with the provisions of the Regulation on the Procedures and Principles Regarding the Regulation of Broadcasts Made on the Internet Environment and the Regulation on the Procedures and Principles Regarding the Issuance of Activity Certificate to Access Providers and Hosting Providers by The Telecommunication Authority.

30. Social Media – What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable online safety laws?

Obligations related to online safety are regulated under various separate legal instruments, each setting forth specific rules for different types of service providers and content. For example, pursuant to Article 1-b/4 of the Regulation on Administrative Sanctions of the Information and Communication Technologies Authority, operators that fail to meet internet safety obligations may be fined up to 1% of their net sales from the preceding calendar year. In addition, publicly disseminating false or misleading information is criminalized under Article 217/A of the Turkish Penal Code No. 5237 and is punishable by imprisonment for a term of one to three years.

31. Spatial Computing – Please summarise the principal laws (present or impending), if any, that govern spatial computing, including a brief explanation of the general purpose of those laws?

As of today, Türkiye does not have a comprehensive legal framework exclusively governing spatial computing technologies such as augmented reality (AR), virtual reality (VR), extended reality (XR), or the Metaverse. However, depending on the specific context and application, several existing legal regimes may apply indirectly—particularly in the areas of data protection, consumer protection, and internet law.

The primary legal instrument relevant to spatial computing is the Law on the Protection of Personal Data No. 6698 ("**LPPD**"). Devices commonly used in AR/VR/XR environments —such as VR headsets, biometric sensors, eye-tracking tools, and motion capture systems—process a wide range of personal data including voice, facial expressions, gaze patterns, posture, location, and behavioural metrics. Many of these data types qualify as special categories of personal data under Turkish law, requiring explicit consent in most cases and heightened security safeguards. As such, spatial computing technologies fall under the scope of Türkiye's data protection obligations, with the aim of mitigating privacy risks and safeguarding users' personal data.

In commercial applications (e.g., AR-based retail), the provisions of Law No. 6502 on Consumer Protection may apply, particularly in contexts involving transactions with end-users. Relevant obligations include the right of withdrawal, pre-contractual transparency obligations, and liability for defective or non-conforming digital services. Additionally, depending on the context in which these technologies are deployed, e-commerce regulations may also govern aspects such as digital advertising, and contract formation through spatial interfaces.

Furthermore, under Law No. 5651 on Regulation of Broadcasts via Internet and Prevention of Crimes Committed through Such Broadcasts, entities that host or enable user-generated content—characteristically immersive metaverse platforms—may be classified as "hosting providers" or "social network providers" when they facilitate social interaction. Where applicable, such platforms are required to appoint a legal representative in Türkiye, respond to takedown orders within statutory timeframes (24–48 hours), and retain certain traffic and content records in line with domestic data retention rules.

Beyond these areas, spatial computing technologies may also trigger other several regulations relating to ownership and proof of rights over digital assets, intellectual property infringement, and virtual conduct—including potential criminal liability. As spatial

computing and metaverse platforms continue to evolve, they raise complex legal questions that remain either partially regulated or entirely unaddressed under current Turkish law. Accordingly, further legislative developments are expected in the coming years to clarify legal responsibilities, protect users, and establish technological accountability in virtual environments.

32. Quantum Computing – Please summarise the principal laws (present or impending), if any, that govern quantum computing and/or issues around quantum cryptography, including a brief explanation of the general purpose of those laws?

Currently, there is no standalone law in Türkiye that governs quantum computing or its derivative technologies, such as quantum key distribution (QKD) or post-quantum encryption. This means that legal considerations related to quantum computing—such as data integrity, encryption standards, or cryptographic resilience—are addressed within existing, technology-neutral frameworks, if at all. However, quantum technologies have increasingly been recognised in strategic documents and institutional action plans that guide cybersecurity and technology policy. While not legally binding, these initiatives guide public funding, academic collaboration, and long-term technological roadmaps.

Notably, the "**National Cybersecurity Strategy and Action Plan (2024–2028)**", published under the coordination of the Ministry of Transport and Infrastructure, includes quantum security as a forward-looking objective. The strategy specifically calls for the development of guidance documents and public awareness initiatives focused on post-quantum cryptography, aiming to secure national encryption infrastructure against future threats posed by quantum decryption capabilities.

Similarly, the "**2030 Industry and Technology Strategy**" issued by the Ministry of Industry and Technology identifies quantum computing and communication as critical R&D priorities, citing their potential for breakthroughs in computation, imaging, positioning, and national security. In terms of institutional infrastructure, TÜBİTAK BİLGEM established a Quantum Technologies Department in 2023, and in 2025, the formation of the National Quantum Institute was announced. This institute aims to develop Türkiye's first photonics- and superconducting-based quantum computers and promote applications in cryptography and national cybersecurity.

Quantum cryptography, particularly quantum-resistant encryption, is of increasing relevance in the context of national cybersecurity. Although the Cybersecurity Law No. 7545 does not contain explicit provisions regulating quantum cryptography, the law's explanatory memorandum acknowledges that the growing complexity of cyber threats, driven by emerging technologies such as artificial intelligence, blockchain, and quantum computing, necessitated the creation of a unified regulatory framework. While quantum-specific technologies are not explicitly regulated, any systems deployed within critical sectors (e.g., defense, finance, energy) would likely fall under heightened cybersecurity oversight by the Cybersecurity Directorate, particularly regarding encryption standards and key management practices. Additionally, To the extent quantum technologies are used to store, process, or transmit personal data, the provisions of Law on the Protection of Personal Data No. 6698 would also apply.

33. Datacentres – Does your jurisdiction have any specific regulations that apply to data centres?

Türkiye does not have a standalone regulation specifically governing data centres; however, data centre operations are subject to various legal frameworks, particularly in the areas of electronic communications, sector-specific obligations, cybersecurity and data protection requirements.

Pursuant to the Electronic Communications Law No. 5809 and its associated regulations, any entity providing electronic communication services is required to obtain authorisation. Accordingly, data centres must first obtain authorisation from the Information and Communication Technologies Authority prior to commencing operations. Depending on the technical nature of the services and technologies they offer, data centres may also need to obtain additional authorisations, such as the authorisation for internet service provider services and the authorisation for infrastructure management services. While it is common practice for data centres to procure these internet and infrastructure services from third-party providers, in cases where they choose to deliver such services directly, they are obligated to obtain the corresponding authorisations themselves. To obtain authorisation, in addition to submitting the necessary application forms and supporting documentation, data centre operators must also satisfy specific requirements concerning their corporate structure, the scope of their business activities, the criminal records of shareholders and managers, minimum paid-in capital, and a clean

compliance history free of prior regulatory breaches or license revocations

In addition to the general authorisation requirements, several regulated industries—such as banking, telecommunications, electronic payment and insurance—impose sector-specific obligations when their operations involve the use of data centre services. Data centre companies seeking to serve entities in these sectors must comply with applicable regulatory requirements, which may include audit and documentation standards, data security measures, and, in many cases, data localisation obligations that require operational data—sometimes including backups—to be stored within Türkiye.

Beyond these requirements, data centre operations are also subject to the Law on the Protection of Personal Data and its related regulations, as they typically involve the processing of large volumes of data, including personal data. Depending on the contractual and operational framework, data centres may be classified as either data controllers or data processors. In either case, they are required to comply with a range of data protection obligations, including implementing appropriate data security measures and, where applicable, adhering to cross-border data transfer regulations.

34. General – What are your top 3 predictions for significant developments in technology law in the next 3 years?

Considering ongoing global and domestic developments in law and technology, we foresee the following three areas as pivotal for the evolution of technology law in Türkiye over the next three years:

1. Continued Harmonisation of the Law on the Protection of Personal Data with the General Data Protection Regulation

Since its enactment in 2016, aligning Türkiye's Law on the Protection of Personal Data No. 6698 ("**LPPD**") with the EU's General Data Protection Regulation ("**GDPR**") has been a central focus of legislative efforts. Significant amendments were introduced in 2024, marking a major step toward harmonisation. This process is expected to intensify in the coming years.

Official government documents, including the Turkish Presidency's 2025 Annual Program and the 2025–2027 Medium-Term Program, explicitly prioritize full alignment with the GDPR by the fourth quarter of 2025.

2. Implementation of the Cybersecurity Law No. 7545

The enactment of the Cybersecurity Law No. 7545 on 19 March 2025 represents a major milestone. Its full impact will unfold through the adoption of comprehensive secondary legislation throughout the year and beyond.

The Cybersecurity Council is also expected to issue a formal list of critical infrastructure sectors, which will be subject to strict obligations. This new regulatory framework will significantly influence both public and private sector actors as they adapt to evolving cyber threats.

3. Introduction of National AI Legislation Aligned with the EU AI Act

Given AI's transformative role globally, Türkiye is anticipated to introduce its own comprehensive AI legislation within the next three years. Various national stakeholders—including the Turkish Presidency, the Grand National Assembly, and the Turkish Data Protection Authority—have already initiated preparatory work.

The 2025–2027 Medium-Term Program explicitly commits to developing a legal framework in line with the EU AI Act. It is expected that this effort will include both sector-specific regulations and a general framework law mirroring the structure and risk-based approach of the EU AI Act.

35. General – Do technology contracts in your country commonly include provisions to address sustainability / net-zero obligations or similar environmental commitments?

Currently in Türkiye, it is not common for the technology contracts to include provisions regarding sustainability / net-zero obligations or other similar environmental commitments. However, with the recent Climate Law Proposal may require technology contracts to align with the national net-zero emission goal for 2053 of Türkiye. This proposal requires both public and private technological projects to embed sustainability practices, such as reducing greenhouse gas emissions, utilizing renewable energy sources, and integrating circular economy principles. Additionally, it stipulates regarding to the harmonisation to EU the establishment of emission trading systems (ETS) and carbon offsetting mechanisms making it imperative for technology contracts to specify clear environmental obligations and compliance mechanisms.

Additionally, the Information and Communication Technologies Authority recently introduced decison of External Opinion on the Draft Communiqué on Energy Labelling of Smartphones and Tablets and Draft Communiqué on Ecodesign Requirements for Smartphones, Mobile Phones Other Than Smartphones, Cordless Phones and Tablets may envision environmental standards in the technology sector. These drafts specifically require technology providers to adhere to energy labeling, durability, and eco-design criteria in contracts related to smart devices, including smartphones and tablets. This move not only enforces transparency regarding environmental performance but also obliges companies to design products that are environmentally sustainable, repairable, and recyclable, thereby significantly reducing environmental impact.

Contributors

Yücel Hamzaoğlu
Partner
yucel.hamzaoglu@hhklegal.com

Batu Kınıkoğlu
Partner
batu.kinikoglu@hhklegal.com

Melike Hamzaoğlu
Partner
melike.hamzaoglu@hhklegal.com

Nur Güler
Senior Associate
nur.guler@hhklegal.com

Osman Yücel
Managing Associate
osman.yucel@hhklegal.com